REMARKS

The amendments presented herein are generally consistent with those noted in the telephone call of August 15, 2007. Accordingly, entry of this amendment and reconsideration of the pending claims is respectfully requested.

The Office Action, mailed May 24, 2007, considered and rejected claims 1-12, 14-22 and 24-29. The specification was objection to as failing to provide proper antecedent basis for the claimed subject matter.[1] Claim 8 was objected to for minor informalities.[2] Claims 1-12, 14-22 and 24-29 were rejected under 35 U.S.C. § 112, first paragraph, and claims 1-12, 14-22 and 24-29 were rejected under 35 U.S.C. § 112, second paragraph.[3] Claims 1-12, 14-22 and 24-29 were rejected under 35 U.S.C. § 103(a) as being unpatentable over CERT CC, "CERT Advisory CA-2000-02 Malicious HTML Tags Embedded in Client Web Requests" (*CERT-Advisory*) in view of CERT CC, "Understanding Malicious Content Mitigation for Web Developers" (*CERT*) in view of *Wheeler*, Secure Programming for Linux and Unix HOWTO, and further in view of *Sanin* (U.S. Publ No. 2004/0073811).[4]

1. Rejections under 35 U.S.C. § 112, first paragraph

Applicant notes that when a rejection is made under 35 U.S.C. § 112, first paragraph, for failure to comply with the written description requirement, the burden is on the Examiner and the description is presumed to be adequate unless the Examiner provides sufficient evidence or reasoning to the contrary so as to rebut the presumption. (M.P.E.P. § 2163.04). In the present case, the Examiner has clearly failed to meet such a burden.

---

[1] Although not necessary, Applicant has amended the specification to clearly identify terms which were already expressly or implicitly disclosed in the specification. Applicant notes that the purpose of 37 C.F.R. 1.75(d)(1) and M.P.E.P. § 608.01(o) is to clarify claim terminology. The Office Action recites entire limitations and does not provide any guidance as to which, if any, claim terms are not understood by the Office. In any event, Applicant respectfully submits that each term of the claims that could require any interpretation finds its antecedent basis in the specification.

[2] The objection to claim 8 is moot in view of the above claim amendments.

[3] The amendments to the claims recite refraining from executing an HTTP request, and then informing the user of a marker of active content. Applicant respectfully submits that no contradiction can be found under even the broadest reasonable interpretation of the claims, and that the rejection is therefore overcome.

[4] Although the prior art status of the cited art is not being challenged at this time, Applicant reserves the right to challenge the prior art status of the cited art at any appropriate time, should it arise. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status of the cited art.

In particular, when rejection the claims, the Examiner "must set forth express findings of fact which support the lack of written description conclusion, including: (A) identifying the claim limitation at issue; and (B) establishing a *prima facie* case by "providing reasons why a person skilled in the art at the time the application was filed would not have recognized that the inventor was in possession of the invention as claimed in view of the disclosure of the application as filed." Moreover, a simple statement that the Applicant has not pointed out where the new or amended claim is supported is sufficient only where the support is not apparent and the Applicant has not pointed out where the limitation is supported." (M.P.E.P. § 2164.04(I)).

On page 3 of the Office Action, the Examiner summarily rejects claims 1-12, 14-22 and 24-29. The only cited reasoning is that the Applicant has not pointed out where the new or amended claim is supported. The Examiner does not appear, however, to have considered whether the support is apparent, as required. Of equal significance, on page 10 of Applicant's last response (Amendment "C"), Applicant expressly pointed out where the amendments to the claims are supported in Applicant's original application.

Inasmuch as the Examiner has not considered whether the support is apparent, has disregarded Applicant's express direction as to where the claim amendments are supported, and has provided no reasons why one of skill in the art would not have recognized that the inventor was in possession of the invention as claimed in view of the disclosure of the application as filed, Applicant respectfully submits that the Examiner has failed to meet his burden.

2. Rejections under 35 U.S.C. § 112, first paragraph

By this paper, claims 1, 8 and 18 have been amended, and no claims have been cancelled or added.[5] Accordingly, following this paper, claims 1-12, 14-22 and 24-29 remain pending, of which claims 1, 14 and 24 are the only independent claims at issue.

As reflected in the above claim listing, Applicant's claims are generally directed to methods and computer program products for mitigating a cross-site scripting attack. As recited in claim 1, for example, a method to mitigate such attacks includes maintaining, at a server, a list of active markers. A request is also received from a user computer and a first portion of data and a second portion of data, all of the second portion of data being derived from an outside source.

[5] Support for the claim amendments can be found in the express, implied and inherent disclosure of Applicant's original application, including at least the disclosure in paragraphs 7, 8 and 25 of the original application.

A determination is made whether the request includes a marker of active content as identified in the list of active markers, and is performed by examining only the second portion of data (which includes all of the data derived from an outside source). Thereafter, the server refrains from executing any portion of the request when the request includes the marker of active content. The user is then informed that a marker of active content from the list of active markers on the server has been discovered in the request and is requested to resubmit a request. When the resubmitted request is clean of active markers, such as those inserted by an outside source, a response to the resubmitted request is served.

Claim 8 is directed to a similar method in which an HTTP request is made and checked for script constructs, while claim 24 recites a computer program product generally corresponding to the method of claim 8.

While *CERT-Advisory*, *CERT*, *Wheeler* and *Sanin* generally relate to preventing damage from attacks by third parties, Applicant respectfully submits that they fail to disclose or suggest Applicant's invention as reflected in the above claims. For example, among other things, the cited references fail to disclose or suggest wherein determining that a marker of active content exists includes examining only a second portion of data that includes all of the data derived from an outside source, as claimed in combination with the other claim elements. In other words, the cited references fail to disclose that when examining a request, the first portion of data (i.e., data which is not derived from an outside source) is not examined. Indeed, the references disclose and suggest that an entire request is examined.

As disclosed in *CERT-Advisory* and *CERT*, a request received from a client is at least partially processed, even where it contains malicious code. For example, *CERT-Advisory* generally discusses the problem associated with malicious code from a cross-site scripting attack. (pp. 1-2). To address such problems, *CERT-Advisory* notes that web site developers can prevent such attacks by allowing only a limited character set or by filtering data during generation of the output page. (p. 5, ¶ 3-6). For additional details on encoding and filtering, however, *CERT-Advisory* refers to the *CERT* reference.

CERT adds to the discussion in *CERT-Advisory* regarding methods for avoiding damage due to cross-site scripting attacks. As explained in *CERT*, damage from such attacks can be minimized by filtering specific characters out of web pages that contain both text and HTML markup. (pp. 1, 4). For instance, a web page request may be filtered either during the data input

or data output process to ensure that all dynamic content is filtered. (p. 4, ¶ 4). Thus, *CERT* discloses that dynamic content is filtered, and does so regardless of whether the dynamic content is provided by the server or an outside source.

Applicant also respectfully submits that the *Wheeler* reference fails to remedy the deficiencies of *CERT-Advisory* and *CERT*. Indeed, *Wheeler* discloses a general filtering subroutine to remove special characters, but does not disclose that the general subroutine is limited to a server applying it only to data derived from an outside source, as recited in combination with the other claim elements. (*See* §§ 4.10, 6.15-6.15.2.2).

For example, *Wheeler* expressly approves of the filtering method of *CERT-Advisory* and *CERT* and notes that to make a program safe, the "output must be filtered (so characters that can cause this problem are removed), encoded..., or validated." (§ 6.15.2). Such filtering, as described by *Wheeler* entails removing the special or "bad" characters, while leaving valid characters unaffected. (§ 6.15.2.2). Thus, special or bad characters are removed, but *Wheeler* fails to disclose that the valid characters are not examined.

These deficiencies are further highlighted in the *Sanin* reference. In *Sanin* a web service security filter is disclosed which comprises a server-side plug-in and processes HTTP requests before any other Web service plug-in or application. (*Abstract*). In operation, an HTTP request is processed by a filter before it reaches a Web service application. (¶ 22). The filter operates by parsing the HTTP requests into five categories of objects, and inspects the objects, category by category. (¶ 22). In particular, a method is disclosed that loads a group of pattern rules. (¶¶ 28-29). The incoming HTTP request is then parsed according to the objects and the group of pattern rules is applied to the objects. (¶¶ 30-31). If any substring included in the objects matches a predefined pattern, a rule action is taken (e.g., to reject the request as a bad request). (¶¶32-33). If none of the HTTP request objects matches any rule pattern, then the request is passed for further processing. (¶ 40).

Accordingly, in contrast to Applicant's claimed invention, in which a server examines only a second portion of a request, in which the second includes all of the data derived from an outside source), *Sanin* discloses that all substrings in the objects are examined, regardless of whether they include data from an outside source or data from the server. Thus, the cited references, whether considered alone or in combination, fail to disclose each and every element as claimed by Applicant.

In view of the foregoing, Applicant respectfully submits that the other rejections to the claims are now moot and do not, therefore, need to be addressed individually at this time.[6] It will be appreciated, however, that this should not be construed as Applicant 'regarding the cited art or the pending application, including any official notice. Instead, Applicant reserves the right to challenge any of the purported teachings or assertions made in the last action at any appropriate time in the future, should the need arise. Furthermore, to the extent that the Examiner has relied on any Official Notice, explicitly or implicitly, Applicant specifically requests that the Examiner provide references supporting the teachings officially noticed, as well as the required motivation or suggestion to combine the relied upon notice with the other art of record.

In the event that the Examiner finds remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney at (801) 533-9800.

Dated this 15th day of August, 2007.

Respectfully submitted,

RICK D. NYDEGGER
Registration No. 28,651
JENS C. JENKINS
Registration No. 44,803
COLBY C. NUTTALL
Registration No. 58,146
Attorneys for Applicant
Customer No. 047973

RDN:JCJ:CCN:gd
GD0000002021V001

[6] For the record, Applicant notes that the rejection of claims 15-17 is unclear inasmuch as it is rejected as recited above, but further recites "Hidalgo" and "Fielding", which are not made a basis of the present rejection.